SNIP – Transactions Work Group
Transaction Testing Sub Work-Group

Business-to-Business Transaction Set Testing

Version 2

A White-Paper Describing the Recommended Solutions Associated With Transaction Set Testing between Business Partners

The following draft document has been prepared by SNIP (Strategic National Implementation Process) for the express purpose of soliciting industry review and input. All comments received by or before the comment closing date will be considered for inclusion in the associated final document.

SNIP recognizes the critical importance of Industry review and input to the successful implementation of HIPAA. So please take this opportunity to participate and let your voice be heard.

Business-to-Business Transaction Testing White-Paper Purpose and Scope

Purpose and Scope

Purpose

The Testing Sub-Workgroup of the SNIP Transactions Workgroup has identified issues related to the testing between Business Partners, as related to the HIPAA Transaction and Code Sets Final Rule. The purpose of this white paper is to define the types of testing that should take place between Business Partners, to recommend the minimum testing required between Business Partners, and to suggest the best overall testing methods.

Scope

This document is closely related to, and builds upon, a companion document, *Transaction Compliance and Certification* that has also been generated by the Transaction Testing Sub-Workgroup. This *Business-to-Business Transaction Testing* paper discusses testing of Transaction Sets in terms of 'readiness' between some Covered Entities without regard to Certification standings. However, if an Entity has been Certified, this phase of testing will be expedited. This paper will address the same types of testing that are covered in the Certification paper because some aspects are very similar, and will identify where B2B testing goes "one step further".

This white paper will address the following specific testing issues:

1. What are the types of transaction set testing that are needed between Business Partners as they apply to complying with HIPAA Standards?

2. Will the types of testing vary, depending on the previous successes?

3. What should be included in the testing environment of each of the Business Partners?

4. What other issues should be noted regarding successful business-to-business testing?

5. What principles of Project Management and Testing should be included or assumed in the Transaction Testing project?

Overview

HIPAA regulations require most payers and clearinghouses, and many providers change their existing Electronic Data Interchange (EDI) programs in some way. Many Entities will be adding capabilities for new electronic transactions, and most who are currently exchanging one of the Standard Transactions will have to do so in a different format. Since the number of changes to be made is very large, and the timeframe for implementing the new Standard Transaction formats is very short, it is important that everything possible is done to speed up the development process, without sacrificing the quality of the end result.

One of the most time-consuming tasks in the development cycle is the testing process. One way to speed up the testing process is to modify a testing plan that already exists and builds on previous successes, instead of developing one from scratch. Therefore, this paper will outline the testing that should take place between Business Partners, and make suggestions on methods. This will provide Business Partners with a starting point for their testing planning, and will provide them with a common base on which to base testing discussions.

Recommendations

Subtopic 1: What are the types of testing between Business Partners that apply to the testing of the HIPAA Standard Transactions?

Assumptions: Some of the types of testing described below assume that independent certification and compliance testing has been performed prior to performing testing between business partners.

This white paper focuses on the testing which is independent of certification. The *Transaction Compliance and Certification White Paper* is focused on discussing the steps and effort in certification and compliance testing.

It is further assumed that, when all of these types (or an agreed-upon subset of these types) of testing have been completed, then the "sending" entity will be approved for production use with the receiver's system. Finally, testing needs to take place in an environment which is separate from the Production system, but which uses copies of production data files and simulated production-like transaction edits. *Ensure appropriate attention to protecting Patient Privacy.*

Recommended Types of Testing:

In preparation for any testing between Business Partners capacity and volume testing should be completed.

Load / Capacity / Volume – Testing to ensure that the system will not fail because of increased file sizes or increased numbers of transactions. Each entity should simulate the volume of transactions that they estimate will be processed in the production environment. This is particularly important since the translated X12 transactions can be quite large. Examples of aspects that should be checked are temporary file space, batch run times, and capacity of translators or other front-end programs.

Once an entity has established that system changes for HIPAA have accommodated impacts to volumes, etc. test should be performed regarding the physical transmission of files.

Type A: ***Transmission Integrity*** – Testing of the transmission for completeness; testing of the file for valid segments, segment order. This will validate the high level accuracy of the file submission.

Following completion of telecommunication tests which confirm the integrity of transmissions, the Certification and Compliance Testing would be performed. Refer to the *Transaction Compliance and Certification White Paper* for a complete discussion of the types of testing performed for certification, which include:

- Integrity testing
- Requirement testing
- Balancing
- Situation testing
- Code Set testing
- Product Types or Lines of Service

NOTE: If an Entity has been certified by any of the Certifying organizations, then testing should only require a cursory review. *(Refer to the Transaction Compliance and Certification White Paper, Appendix A* for a list of some of the Certification Organizations*.)* **Entities only need to test the lines of service which apply to their organization.** The following types are unique to the specific relationships between Entities:

Type B: Field Lengths - There are some fields that have very long maximum lengths in the X12 standard, where the Business Partner's system may not be able to accommodate the maximum length. HIPAA rules prohibit the rejection of a transaction when they follow the X12 standards, but if a Business Partner's system is continually truncating specific fields, adjustments may need to be made.

Type C: Output - Checking to be certain that output can be produced, and that the output is the type required by the receiver. For example, some providers will want paper remittance advices, while others will want an electronic 835 transaction.

Type D: Security - Testing of specific security-related values that exist between Business Partners. This scenario will be coordinated with the Security and Privacy SubWorkGroup.

Subtopic 2: Will the types of testing vary, depending on the success of previous testing? For example, if a payer has successfully tested incoming claims with a given clearinghouse, should all claims from that clearinghouse be automatically accepted?

Recommendation: The key to knowing whether to test again is determined by whether or not the program that generated the file, or the data content have changed. For example:

- If a Sender is using a Vendor or Clearinghouse to generate a certain transaction, and
- That Vendor/Clearinghouse has already been sending approved files for a specific transaction to the Receiver, and
- The Vendor/Clearinghouse is using the same programs to generate the approved transactions for every Client, or
- A new Sender using the same Vendor or Clearinghouse and with the same or equivalent data content wants to test,

Then no further testing should be required. All Clients of the Vendor/Clearinghouse should be able to send the approved transactions to the Receiver.

It is important to note that even two Senders using the same Clearinghouse may have different data content (e.g., different specialties) thus resulting in different HIPAA transactions. The Vendor or Clearinghouse should ascertain whether both the formatting and the data content requirements for each Sender have been met. For example, a Clearinghouse demonstrating that they can successfully transmit claims for Office Visits, should not automatically assume that they can correctly send Ambulance claims, even though the same software is used.

However, if the Clearinghouse is creating a custom translation program for each Client, and the custom programs create the transactions that are sent to the Receiver, testing would be required each time the custom program is changed.

Subtopic 3: What should be included in the testing environment of each of the Business Partners?

Recommendation: Business Partners should understand the environments that produce the "sent" transactions, and process the "received" transactions during the testing process. This will allow them to correctly devise testing scenarios, and to assess the risks that exist when the transactions are put into production.

The overall rule for the testing environment is to use production versions of programs and table files. In addition, testing should not be considered complete until data is processed all the way through the life-cycle of the transaction. For example, claims testing should go all the way through to the check "print", printing on voided checks or on blank paper.

Privacy for patient information must be carefully evaluated when submitting tests between Business Partners. Many covered entities, before implementing HIPAA, would use "live" data for testing. A balance must be maintained between patient confidentiality and testing that is thorough enough to ensure success when the transactions are approved for "live" use. One suggestion is to use altered or fictitious patient information for everything but the final test run. Another suggestion is to make sure that the receiving Business Partner knows exactly when actual patient information is being used, and to agree to quickly destroy the test files after the testing is complete.

A "beta test" process should be put in place for each transaction set, without regard to whether it is a "sending" and "receiving" business entity. This first or trial test process is usually executed between highly-trusted partners. The partners agree to very high

levels of data quality exchange, so that the programs/transactions on both sides will be thoroughly tested before expanding the process to the rest of their world.

Subtopic 4: Are there other issues related to transaction testing, that are required for successful testing and "move to production" of each of the transactions?

Recommendations: Every effort must be made to ensure the protection and security of Patient Identifiable Information during this testing process. Ideally, the Security and Privacy measures also defined under HIPAA will be developed and in place in time to be executed during this transaction set testing.

Subtopic 5: How could the principles of Project Management and Testing be included in the Transaction Set Testing project?

Recommendations:

a. ***Project Planning:*** Implementing the Transaction Sets using the HIPAA standard in the legislated timeframes is an immense project. While all projects need planning, the larger the project and the more aggressive the Milestone Dates, the need is more critical. The following are some of the activities involved in the Project Planning Phase:

- Develop estimates to perform the work
- Define a physical plan for completing the work
- Identify and document phases of the project's lifecycle, including the conclusion and transition to Production support
- Estimate costs and initiate budget
- Estimate and assign resources
- Review technical environment resources for capacity planning
- Determine a method to identify, resolve and document risks
- Obtain the support and commitments from the affected management, Customers and Partners for the project's structure, objectives, resources and budgetary obligations.

b. ***Project Tracking and Communication:*** This area of the project is to provide visibility into the progress of the actual work to management, Customers and Partners. Project Tracking and Communication involves monitoring, reviewing presenting the results. This area compares actual results against the physical plan, estimates, commitments and dates; adjusts the plan as appropriate; and communicates the results and revisions.

Especially because the objective of this project is to provide an electronic alternative for current processes, particular attention is needed in the area of Communication with Customers and Business Partners. For example, if a Provider currently submits HCFA1500 documents for billing professional services the Payer should verify the Provider's submission preference after October 16, 2002. If Providers currently have no options and only receive paper Remittance

Advices, the Payer should conduct a survey to determine which Providers prefer electronic 835s.

Periodic status meetings which include representatives from all the affected areas and enterprises should be considered. These meetings would provide the ability coordinate and perhaps consolidate, the following items, which each enterprise should be monitoring.

The following are some of the tasks to be considered in Project Tracking and Communication:

- Project schedule, monitoring and maintenance
- Issue/Action Item tracking and reporting
- Risks associated with budgets, commitments, dates, scope, resources, technical environment monitoring and reporting
- Tracking of Technical issues and corrective actions including acquisition and performance
- Define Inter-group Coordination and Communication
  - Management Communication
  - Customer Communication
  - Business Partner Communication
  - Status Reporting

c. ***Product Engineering (Development Coding and Unit Testing):*** This area of the project is familiar to most everyone. Documenting changes and design specifications that need to be made; performing the coding changes and unit testing to ensure the changes function. Map to the appropriate fields and create the proper segments, records, envelopes, etc.

d. ***Change Management / Version Control:*** This area of the project may need special consideration and control because the purpose of the HIPAA legislation is to standardize nine types of electronic transactions. It relates to creating and accepting inbound and outbound data, however this may be a project that is prone to what some refer to as “scope creep”. Making sure that the inbound or outbound data is correctly formatted into a transaction, could lead to the way that data is processed by the Payer’s Administrative system. The intent of HIPAA legislation was not to mandate enhancements to a system’s processing capabilities or functionality.

Safeguards should be put in place to ensure that formatting a claim into an 837 layout, for example, is not allowed to creep into adding functionality to process Workers’ Compensation claims in an Administrative system that currently lacks that functionality.

Another function of Change Management is system defect tracking. This is not the function that identifies and records the defects / problem reports. It is the area that monitors tracks and reports the volume (for example, New this reporting period, In Process, Resolved this reporting period, etc.) Efforts should be made to analyze the reported defects in order to initiate defect prevention. Providers, Clearinghouses and Payers will all be repeatedly creating and transmitting or receiving and processing these Transactions. For example, Providers may be submitting files to multiple Payers; Clearinghouses will be receiving files from multiple Providers and creating files for multiple Payers; etc. Initiating a defect

prevention process or 'lessons learned review' will allow updates to the implementation process which should make the work with the next Provider or Clearinghouse or Payer go more smoothly.

e. ***Configuration Management / Operations Support:*** Configuration Management systematically controls changes to the elements that define "The System". This area systematically maintains the integrity and traceability of The System throughout the project's lifecycle.

While the Configuration Management function controls the delivery of software to a Customer, the Operations Support function controls receipt of electronic media from a Customer. The practices and procedures used in Operations Support are of critical importance to this project especially for the Clearinghouses and Payers that will be receiving and initially processing the electronic media.

f. ***Transaction / System Testing:*** Systems Testing is a group of individuals who have the responsibility for planning and executing independent, user oriented testing of the system to ensure that the changes perform according to specifications and requirements and that the system as a whole was not adversely affected by the changes.

g. ***Resource and Budget Management:*** This area defines all projects, but special consideration should be given to:

- Training
- Documentation
- Transmission Guide
- On-Site Support
- Customer Service Support
- Technical On-Call Support
- Transition to Production Support

h. ***Lessons Learned / Post-Implementation Review:*** This area considers how to improve the process, especially when faced with a phased implementation approach. The implementation of HIPAA Standard Transactions will be based on a national sequence so lessons can be learned to improve the next transaction implementation. For Payers, Clearinghouses are urged to consider utilizing a phased approach with converting Providers to the new transactions. Therefore one entity's implementation of each transaction set will allow lessons learned sessions to improve the process for the next test.

Value in Accepting

The value in accepting these recommendations will be to provide guidance to health plans, healthcare providers, and clearinghouses regarding the testing process. By following these recommendations it is expected that communication between Business Partners will be improved, thereby aiding in the implementation of the HIPAA Standard Transactions in a timely fashion.

Test Plan Summary

Appendix A is a document that provides a Plan Outline for the Testing Process. This Outline

may provide a summary view and a visual ‘how-to’ guide to apply the previous information.

APPENDIX A
MODULAR REPEATABLE PROCESS FOR TESTING

TEST PLAN

Note: All task steps may not always be performed. Test requirements will dictate which steps will be performed. This a general out line containing examples.

1.0 Test Functions

1.1 Testing Resources:

Who:	Deliverables:	Tools:
[Areas responsible for testing]	Test I/O requirements document Test results document.	*[list of tools}*

Tasks:

1. Identify the computing environment to be assigned to complete the test.
   - Determine degree of testing required
   - Determine security criteria (Internal/External)
   - Determine Hardware/Software testing environment setup
     - ⇒ Mainframe
     - ⇒ Client/Server
   - Determine Internal/External Architecture connectivity
     - ⇒ Networks
       - * Internet
       - * Intranet
       - * Cross Platform (such as mainframe to client/server connectivity)
   - Identify all Input /Output data resources
   - Identify Input/Output space criteria
   - Identify processing tools used for validation of test.
   - Determine issue tracking and resolution process procedures, reporting and setup
   - Determine Status reporting required by management (weekly, monthly, quarterly)
   - Determine Version Management process

2. From the test classification and environment above, determine all staffing support responsibility for test;

Examples of resource types that will be needed for the test process

- Network Administration Functions
  - ⇒ Define and validate network connectivity (Software and Hardware)
  - ⇒ Monitor volumes across network
  - ⇒ Audit and log errors and issues associated with network performance
- Security Administration Functions
  - ⇒ Setup security based on business needs (data, network access)
  - ⇒ Monitor and audit security access based on test
- Staff test team members and responsibility
  - ⇒ **Team Lead** - Coordinate, construct, analyze, validate, and assist in all testing efforts provide technical support / analysis for prep team, validate test environment and establish staffing needs
  - ⇒ **Project Analyst** - Assist Team Lead with validation of inventory, review of testing/procedures/setup
    - * control cards, known error conditions, screens and reports and resolving issues, problems and concerns. Attend Subject Matter Expert interviews, prepare actual vs expected results
    - * documentation, error and problem reporting.
  - ⇒ **Senior Tester** - Create testing documentation, identify, coordinate, construct, analyze and validate test scripts. Assign testers according to testing needs

    Support and assist other team member and provide continuous support to testers.
  - ⇒ **Tester** - Execute scripts, verify results, error problem solving, update test script documentation, release to acceptance testing and sign off. Testing activities are:
    - ◊ Produce test processes
    - ◊ Test documentation
    - ◊ Test execution
    - ◊ Test verification
    - ◊ Testing problem reporting
    - ◊ Applying retrofits
- Preparation Teams Functions

⇒ Provides a verified list of components to be tested

- Support for testing consist of:
  - ⇒ Subject Matter Expert (SME) will verify:
    - ∗ Input /Output components
    - ∗ Scheduling requirements
    - ∗ Confirm level of testing needed (as indicated on Test Processes and Test Scripts)
    - ∗ Review Test Plan
    - ∗ Review Batch Process and On-line Process
    - ∗ Review all Batch Scripts and all On-line Scripts
    - ∗ Identify known error conditions associated with each system
- Pre-Test Preparation Team will be required in verifying and building test environment:
  - ⇒ Determine all related files for each system
  - ⇒ Finalize the frequency and run order for all jobs
  - ⇒ Determine duplication
  - ⇒ Identify programs that update the subsystem databases
  - ⇒ Determine space requirements
  - ⇒ Verify all files have been moved from production to test environment
  - ⇒ Provide all backup / restore capabilities
  - ⇒ Coordinate component moves
  - ⇒ Test configuration setup
  - ⇒ Verify the test environment is stable for test execution
  - ⇒ Support the tests team with system ABENDs, errors, etc.
- Data Base Administration Functions
  - ⇒ Will create necessary backup and restore capabilities for data bases
  - ⇒ Will provide mechanisms to populate databases across environments
- Version Control Administration Functions
  - ⇒ Monitor version control process
  - ⇒ Determine process of version control based on platforms used.
- Testing Administration Functions
  - ⇒ Update issues and resolutions associated with testing
  - ⇒ Determine resources to resolve issues
  - ⇒ Prepare status reporting for management (weekly, monthly, quarterly)

1.2 Test Input/Output Requirements:

Who:	Deliverables:	Tools:
[Areas responsible for testing]	Test I/O requirements document Test results document.	*[list of tools}*

Tasks:

1. Identify input requirements necessary to fully perform the test.
   - Validate inventory of all load components, parameters and procedures required to perform the test
   - Review and validate all Input and data set allocations,

2. Identify known predictable data errors for the test to ensure that the system can correctly handle error conditions. Where applicable , the team will initialize the input data back to its original configuration to facilitate repetitive testing. The Team will:
   - Validate error conditions are present and that input data will cause error condition,
   - Review all previous Test results for completeness before using updated programs,
   - Review and update if necessary the documented expected results of the test.

3. Identify expected outputs from the test that will be used to help validate the functionality of the changes made to the programs and supporting areas identified as part of the test. The Team will
   - Review and validate all Output files and data set allocations,
   - Identify all output files and their use in the expected results evaluation,
   - Identify all output reports and their use in the expected results evaluation,
   - Review planned error conditions and document the expected effect and or results,
   - Identify data file manipulations
   - Document expected effect that changes will have on screen images,
   - Document all issues and their resolution.

1.3 Testing Processes:

Who:	Deliverables:	Tools:
[Areas responsible for testing]	Test plan. Test results document.	*[list of tools}*

Tasks:

1. The Team will perform the following test procedures using established standards:

   - Identify the subsystems that constitute final testing:

Examples Of subsystems that would be tested together (Integration testing)

   ⇒ Electronic Data Interchange (Inputs/Outputs)

   ⇒ Enrollment System (Inputs/Outputs)

   ⇒ Regular Business Membership System (Inputs/Outputs)

   ⇒ Group Subscriber System (Inputs)

   ⇒ Entry Suspense System (Inputs/Outputs)

   ⇒ Special Claims System (Inputs/Outputs)

   ⇒ Common History System (Inputs/Outputs)

   ⇒ Common Check Writing (Inputs/Outputs)

   - Execute test scripts using defined requirements from the Test Plan,
   - Identify and communicate problems and their recommended resolutions to Project Control,
   - Validate actual results to expected results and document deviated results,
   - Where applicable, initialize the input data back to its original configuration to facilitate repetitive testing.

2. The following items must be identified and procedurally controlled during all testing phases:

   - Procedures
   - System Libraries (Source code, Object code, Copybooks)
   - Test Script
   - Test data/dates
   - Input files
   - Output files

1.4 Testing Documentation:

Who:	Deliverables:	Tools:
[Areas responsible for testing]	All documents listed in this section.	*[list of tools}*

Tasks:

1. The Test documentation must support the certification that the changes was tested and no problems identified as critical remain unresolved.

Examples of types of documentation that would be needed for the test process.

- Analysts status report (Analyze Status)
- Listing of Component files (Component Listing)
- Cycle Testing (Cycle Testing Schedule)
- Job Stream Schedule (Job Schedule)
- List of input and output files (Input/Output)
- SME turnover acceptance checklist (Acceptance)
- Job Control Cards (Job Control Card Attachment)
- List of reports (Reports Attachment)
- Return Codes for all error messages/error conditions (Return Codes Attachment)
- Notification of acceptance stage of completion (Acceptance Awareness Letter)
- Acceptance process checklist (Acceptance Checklist)
- Planning and control issues (P&C Notification of Issues)
- Notification of start of testing (Test Awareness Letter)
- SME questionnaire responses (Test Questionnaire)
- Testing status information (Task Team Checklist)
- Detailed job trigger information (Documentation Library)
- Report of documented questions and problems (Issues)
- Test documentation and preparation status (Test Preparation and Status Checklist)
- Test Plans (Test Plans)
- Test Processes (Test Business Processes)
- Test Scripts (Test Scripts)

APPENDIX B
ACKNOWLEDGEMENTS AND DISCLAIMER

Acknowledgments

The SNIP Transaction Set Testing SubWorkGroup is comprised of organizations from all facets of the Health Care Industry. The following list represents many of the organizations participating in this Testing SubWorkGroup. The Members of these organizations which have volunteered their time and energies are greatly appreciated and acknowledged.

BlueCross/BlueShield of Florida
BlueCross/BlueShield of Kansas
CIGNA
California Association of Health Plans
California Department of Health Services - with special thanks to Karen Weber, co-writer of this document
Claredi
The Cleveland Clinic
Complete Business Solutions, Inc.
Electronic Data Systems
Empire Medicare Services
GE Global Exchange Services, Inc.
HDX
Health Care Finance Administration
IDX
IHC
John Muir / Mt Diablo Health System
McKessonHBOC
Mayo Clinic
Missouri Medicaid
New Era of Networks Inc.
State Farm Insurance Companies
Washington Department of Health Services
Verizon, Inc. - with special thanks to Marsha Solomon, co-writer of this document

Disclaimer

The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice / recommendations by the Workgroup for Electronic Data Interchange, nor the SNIP Transaction Set Testing SubWorkGroup. This SubWorkgroup presents information that its members are aware of, without implying that surveys or other formal evaluations were performed in order to create information presented in this document. Nor does the listing of an organization in this document imply any sort of endorsement by the Workgroup for Electronic Data Interchange. The Workgroup for Electronic Data Interchange takes no responsibility for the products or tools offered by the organizations referenced in this document.